EXHIBIT G

Windows NT™ MAGAZINE

RealSecure 1.0 for Windows NT

Monitor your network and protect it from malicious attacks

Intel MIPS Alpha PowerPC

RealSecure 1.0 for Windows NT

Contact:
Internet Security Systems • 770-395-0150
Web: http://www.iss.net

Price: $4995 for a single perpetual license

Attacks on networks connected to the Internet are rampant and getting worse. People are continually discovering new ways to break into or disable Windows NT. You are justified in protecting your network, but you need tools to do the job. One gem of a network protection tool is RealSecure 1.0 for Windows NT, from Internet Security Systems (ISS).

You might think your network is protected adequately, but how do you know for sure? Do you know when someone is trying to break in or attack a network service? Maybe you monitor the attack logs that your security systems produce. Although monitoring system logs is a great practice, it doesn't stop attacks; it simply informs you that an intrusion occurred.

Not all security systems can recognize all forms of attacks. Frequently, you have to program a security system with information about an attack type before it can prevent or detect it. The security system you bought last year might not adequately handle this year's attack methods. The solution is to keep your security systems up-to-date, a time-consuming but worthwhile effort.

Between updates to your security systems, RealSecure, a realtime network attack recognition system, can help you monitor network security. RealSecure looks at network traffic at the packet level (much like a network sniffer) and uses its built-in attack recognition logic and definable filtering rules to determine whether the packets are potentially malicious. (RealSecure can recognize more than 200 different system attacks.) Filter rules define the action to take when RealSecure detects an attack. When it finds suspicious packets, RealSecure can record the date, time, source, and target of the event; record the event's content for session playback; notify administrators of the attack; or terminate the attack by killing the affected network sessions. Powerful stuff, to say the least.

Inside RealSecure

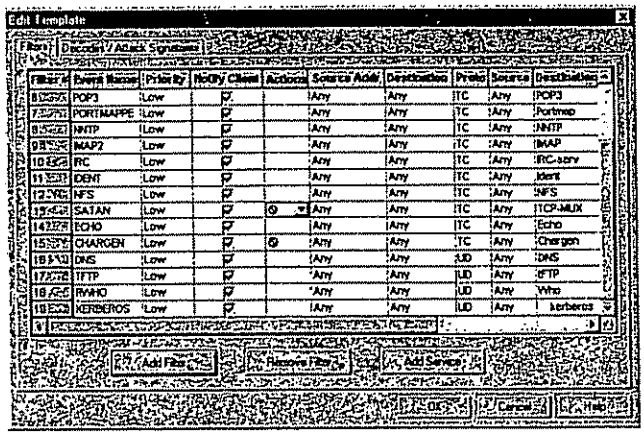
Let's take a quick look at RealSecure's components to see how they interact. RealSecure installs as an application console, a network service (which ISS calls an *engine*), and a custom packet driver that you load with your other network protocols.

The RealSecure engine reads the packets as they arrive at the network interface from the packet driver. The engine compares the packets to established filtering rules. If the engine finds a packet that matches a rule, the engine's attack recognition logic parses the packet information. If the logic detects an attack, the engine takes an appropriate action as defined in the filtering rules. The engine also sends all packets that match the filters to the console for logging, reporting, session playback, or review.

Installation and Configuration

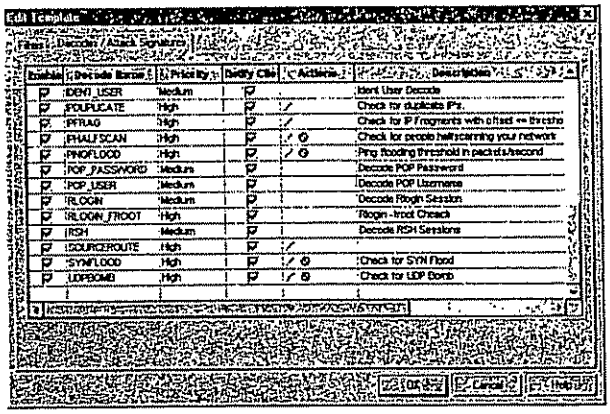
Installing the software is quick and painless. You need to install the software on each segment that you want to monitor. You can load a packet driver and engine on an NT system residing on each remote segment and then load a single centralized console on an NT system that collects data from the other RealSecure engines. If your network is simple (i.e., it uses only one network segment), you can load one copy of RealSecure on any NT box to monitor your entire LAN. Each console uses an authenticated and encrypted system-to-system session to talk with a remote engine. This process prevents any tampering with your RealSecure monitoring system's network traffic.

After you've installed RealSecure on each system, you fire each one up and configure it. Configuring RealSecure means defining which attacks or suspicious activity you'd like to watch out for (called *filtering*) and what to do about a particular event when RealSecure detects it. For example, if your network security policies disallow all inbound Telnet sessions and you've adjusted your firewall to prevent them, you could configure RealSecure to watch for

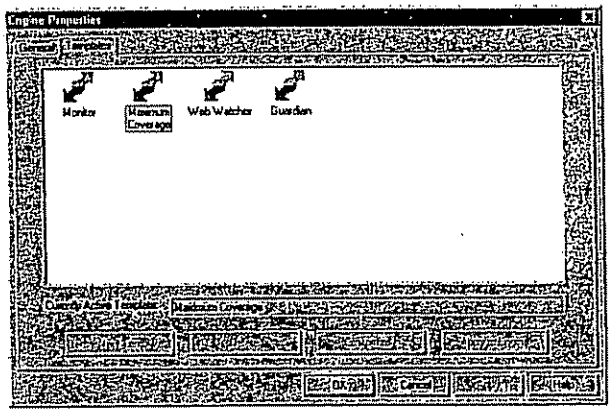


▶ SCREEN 1: Displaying the filter logic of the Maximum Coverage template

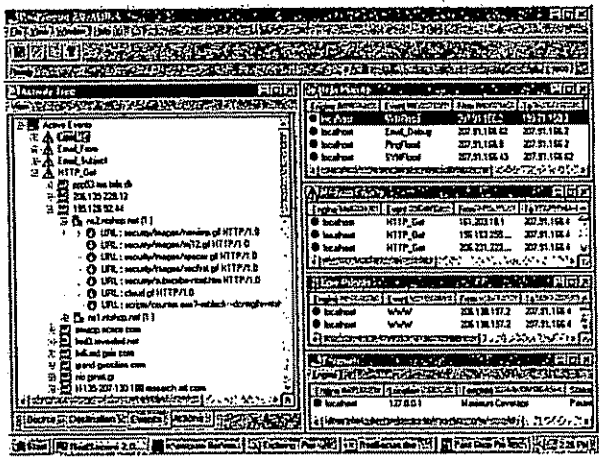
▶ SCREEN 2:
Viewing the engine's attack signatures



▶ SCREEN 3:
Selecting a filtering profile



▶ SCREEN 4:
Viewing RealSecure's console interface



inbound Telnet connections. If an intruder defeats your firewall and launches a Telnet session, RealSecure can detect the session, shut it down immediately, and record a detailed log of what occurred during the session.

RealSecure can recognize hundreds of potential attack scenarios. Screen 1 shows some predefined filter logic of the Maximum Coverage template; Screen 2 shows some attack signatures used for detection in the attack recognition portion of the engine. You can use the built-in templates or define your own.

After you configure the software, you assign your chosen filter profiles to each engine on your network. To assign filters to an engine, right-click an engine listed in the Engine window, choose Properties, select a filtering profile from the choices (as you see in Screen 3), and click Apply to Engine. The engines start up using the specified filters and begin acting as your network watchdogs. You can manage all engines, local and remote, from one centralized console, which simplifies management in a distributed environment.

RealSecure in Action

RealSecure's console is the central place where you review the captured suspicious network activity. As you see in Screen 4, the interface has five windows. In the left window, you can see a hierarchical view of the source address, the destination address, events, or actions taken on those events. This window's NT Explorer-style tree view provides an easy way to drill down to the capture information. The three top windows on the right (High Priority, Medium Priority, and Low Priority) display each type of captured event according to its definable priority level. The Engine window identifies the location of the engine and the template being used for monitoring.

Screen 5 shows a maximized view of the Medium Priority event window. As you can see, RealSecure has captured many events that I defined in the filters as being of medium concern to me. These events are mainly HTTP_Get requests, the usual request a Web browser uses to retrieve a Web page. RealSecure captured the name of the engine reporting the event, the Web Get request, the user's IP address (source address), the destination address (my Web servers' addresses), the URL used to retrieve the document or file, and the time and date. Ordinarily, you don't want to monitor every user retrieving simple Web pages from your server, but I do because my Web site has encountered suspicious activity in the past. Tracking all access might help me catch an intruder red-handed.

High-priority events are the most interesting. During my test, I launched many attacks (ping floods, SYN floods, IP spoofs, User Datagram Protocol bombs, and several other common intrusion attacks) on my systems to see how RealSecure would react (as shown in Screen 6). As I expected, RealSecure immediately detected my attacks, collected information about them for my review, and shut them down.

Another nice feature of RealSecure is its ability to capture and replay entire network sessions. For example, you can define a filter to track and capture

attempts to Telnet into your router or other systems. Later, you can replay the session to see what the intruder was doing. You can use these captured sessions as evidence against the would-be intruder if you prosecute. Really slick and greatly needed.

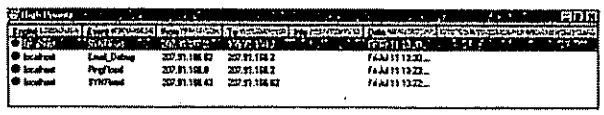
The software is robust and easy to use, and it has plenty of useful features. A report generator produces formatted reports. And the ISS support team does a fantastic job of answering your questions.

The second major release of RealSecure will contain new functionality such as automatic attack logic updates over the Internet and the ability to push RealSecure out to remote servers without special software such as Microsoft's Systems Management Server (SMS). RealSecure runs on NT and on a variety of UNIX operating systems, and the program can detect attacks against any operating system using TCP/IP, not just NT.

I want to point out that someone could misuse RealSecure's power internally to launch attacks against your network. For instance, just as you can use RealSecure or some other software to prevent users from surfing to certain Web sites, disgruntled employees could use RealSecure to attack your network or wreak havoc on connecting networks. Treat the tool like any other sensitive information or equipment: Limit access so that only trusted operators can get to the RealSecure consoles. In the next version of RealSecure, ISS will add a feature that lets RealSecure detect other copies of RealSecure on the network; this feature will help control internal misuse of the software.

I'm impressed with this new product, and I feel much more secure about my LAN environment now that I have it installed and running. RealSecure is a must-have package for any serious network environment, especially if you're connected to untrusted networks such as the Internet.

◀ SCREEN 5: Displaying a Medium Security events window



◀ SCREEN 6: Viewing active attacks

ABOUT THE AUTHOR

Mark Joseph Edwards is a writer and network engineer with more than 16 years of experience in network engineering and communications. He is the news and UPDATE editor for Windows NT Magazine, *founder of Netropolis Technology Group (NTg), and author of* Internet Security with Windows NT, *forthcoming from Duke Press. You can reach him at*

ISS_02125874

Internet Security Systems, Inc. (ISS)
41 Perimeter Center East
Atlanta, GA 30346
Phone: 770-395-0150
Phone: 800-776-2362
Fax: 770-395-1972
Email: iss@iss.net
www.iss.net